Listing of the claims

1-174. (Cancelled)

175. (New) A method of redirecting data items from a messaging host system to a user's mobile device, comprising the steps of:

establishing a secure communications link between a redirector host system and the user's mobile device;

generating a first encryption key at the redirector host system;

storing the first encryption key at the redirector host system;

generating a first decryption key at the redirector host system;

forwarding the first decryption key from the redirector host system to the user's mobile device using the secure communications link;

detecting a new data item for the user at the messaging host system by the redirector host system;

receiving a copy of the new data item at the redirector host system;

determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

if the new data item should be redirected, then encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

transmitting the encrypted new data item from the redirector host system to the user's mobile device.

176. (New) The method as recited in claim 175, wherein the step of establishing a secure communications link between a redirector host system and the user's mobile device further comprises establishing a serial connection between redirector host system and the user's mobile device.

177. (New) The method as recited in claim 175, wherein the step of establishing a secure communications link between a redirector host system and the user's mobile device further comprises using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

178. (New) The method as recited in claim 175, wherein the steps of generating a first encryption key at the redirector host system and generating a first decryption key at the redirector host system further comprise generating a shared key.

179. (New) The method as recited in claim 175, wherein the first encryption key and the first decryption key are generated according to a symmetric key encryption scheme.

180. (New) The method as recited in claim 175, wherein the step of generating a first encryption key at the redirector host system further comprises generating a public key.

181. (New) The method as recited in claim 180, wherein the step of generating a first decryption key at the redirector host system further comprises generating a private key.

182. (New) The method as recited in claim 175 further comprising the steps of:

receiving the encrypted new data item at the user's mobile device; and

decrypting the encrypted new data item to recover the new data item using a cipher algorithm and the first decryption key.

183. (New) The method as recited in claim 182 further comprising the step of storing the new data item within a memory of the user's mobile device.

184. (New) The method as recited in claim 182 further comprising the steps of:

generating a second decryption key at the redirector host system;

storing the second decryption key at the redirector host system;

generating a second encryption key at the redirector host system; and

forwarding the second encryption key from the redirector host system to the user's mobile device using the secure communications link.

185. (New) The method as recited in claim 184, wherein the steps of generating a second encryption key at the redirector host system and generating a second decryption key at the redirector host system further comprise generating a shared key.

186. (New) The method as recited in claim 184, wherein the second encryption key and the second decryption key are generated according to a symmetric key encryption scheme.

187. (New) The method as recited in claim 184, wherein the step of generating a second encryption key at the redirector host system further comprises generating a public key.

188. (New) The method as recited in claim 187, wherein the step of generating a second decryption key at the redirector host system further comprises generating a private key.

189. (New) The method as recited in claim 184 further comprising the steps of:

preparing a reply data item at the user's mobile device that is related to the new data item;

encrypting the reply data item at the mobile device to form an encrypted reply data item using a cipher algorithm and the second encryption key; and

transmitting the encrypted reply data item to the redirector host system.

190. (New) The method as recited in claim 189 further comprising the steps of:

receiving the encrypted reply data item at the redirector host system;

decrypting the encrypted reply data item to recover the reply data item; and

transmitting the reply data item to the messaging host system.

191. (New) The method as recited in claim 190 further comprising the step of transmitting the reply data item to a destination system using an electronic address associated with the user at the messaging host system, wherein reply data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.

192. (New) A system for redirecting data items from a messaging host system to a user's mobile device, comprising the steps of:

means for establishing a secure communications link between a redirector host system and the user's mobile device;

means for generating a first encryption key at the redirector host system;

means for storing the first encryption key at the redirector host system;

means for generating a first decryption key at the redirector host system;

means for forwarding the first decryption key from the redirector host system to the user's mobile device using the secure communications link;

means for detecting a new data item for the user at the messaging host system by the redirector host system;

means for receiving a copy of the new data item at the redirector host system;

means for determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

means for encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

means for transmitting the encrypted new data item from the redirector host system to the user's mobile device.

193. (New) The system as recited in claim 192, wherein the means for establishing a secure communications link between a redirector host system and the user's mobile device further comprises a serial connection between redirector host system and the user's mobile device.

194. (New) The system as recited in claim 192, wherein the means for establishing a secure communications link between a redirector host system and the user's mobile device further comprises means for using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

195. (New) The system as recited in claim 192, wherein the means for generating a first encryption key at the redirector host system and the means for generating a first decryption key at the redirector host system further comprise means for generating a shared key.

196. (New) The system as recited in claim 192, wherein the means for generating a first encryption key at the redirector host system and the means for generating a first decryption key at the redirector host system further comprise means for generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

197. (New) The system as recited in claim 192, wherein the means for generating a first encryption key at the redirector host system further comprises means for generating a public key.

198. (New) The system as recited in claim 197, wherein the means for generating a first decryption key at the redirector host system further comprises means for generating a private key.

199. (New) The system as recited in claim 192 further comprising:

means for receiving the encrypted new data item at the user's mobile device; and

means for decrypting the encrypted new data item to recover the new data item using a cipher algorithm and the first decryption key.

200. (New) The system as recited in claim 199 further comprising means for storing the new data item within a memory of the user's mobile device.

201. (New) The system as recited in claim 199 further comprising:

means for generating a second decryption key at the redirector host system;

means for storing the second decryption key at the redirector host system;

means for generating a second encryption key at the redirector host system; and

means for forwarding the second encryption key from the redirector host system to the user's mobile device using the secure communications link.

202. (New) The system as recited in claim 201, wherein the means for generating a second encryption key at the redirector host system and the means for generating a second decryption key at the redirector host system further comprise means for generating a shared key.

203. (New) The system as recited in claim 201, wherein the means for generating a second encryption key at the redirector host system and the means for generating a second decryption key at the redirector host system further comprise means for generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

204. (New) The system as recited in claim 201, wherein the means for generating a second encryption key at the redirector host system further comprises means for generating a public key.

205. (New) The system as recited in claim 204, wherein the means for generating a second decryption key at the redirector host system further comprises means for generating a private key.

206. (New) The system as recited in claim 201 further comprising:

means for preparing a reply data item at the user's mobile device that is related to the new data item;

means for encrypting the reply data item at the mobile device to form an encrypted reply data item using a cipher algorithm and the second encryption key; and

means for transmitting the encrypted reply data item to the redirector host system.

207. (New) The system as recited in claim 206 further comprising:

means for receiving the encrypted reply data item at the redirector host system;

means for decrypting the encrypted reply data item to recover the reply data item; and

means for transmitting the reply data item to the messaging host system.

208. (New) The system as recited in claim 207 further comprising the means for transmitting the reply data item to a destination system using an electronic address associated with the user at the messaging host system, wherein reply data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.

209. (New) A computer-accessible medium having a sequence of instructions which, when executed by a processing entity, effectuate redirection of data items from a messaging host system to a user's mobile device, the computer-accessible medium comprising:

a code portion for establishing a secure communications link between a redirector host system and the user's mobile device;

a code portion for generating a first encryption key at the redirector host system;

a code portion for storing the first encryption key at the redirector host system;

a code portion for generating a first decryption key at the redirector host system;

a code portion for forwarding the first decryption key from the redirector host system to the user's mobile device using the secure communications link;

a code portion for detecting a new data item for the user at the messaging host system by the redirector host system;

a code portion for receiving a copy of the new data item at the redirector host system;

a code portion for determining whether the new data item should be redirected from the redirector host system to the user's mobile device;

a code portion for encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the redirector host system; and

a code portion for transmitting the encrypted new data item from the redirector host system to the user's mobile device.

210. (New) The computer-accessible medium as recited in claim 35, wherein the code portion for establishing a secure communications link between a redirector host system and the user's mobile device further comprises a code portion for establishing a serial connection between redirector host system and the user's mobile device.

211. (New) The computer-accessible medium as recited in claim 35, wherein the code portion for establishing a secure communications link between a redirector host system and the user's mobile device further comprises a code portion for using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

212. (New) The computer-accessible medium as recited in claim 209, wherein the code portions for generating a first encryption key at the redirector host system and generating a first decryption key at the redirector host system further comprise a code portion for generating a shared key.

213. (New) The computer-accessible medium as recited in claim 209, wherein the code portions for generating a first encryption key at the redirector host system and generating a first decryption key at the redirector host system further comprise a code portion for generating the first encryption key and the first decryption key according to a symmetric key encryption scheme.

214. (New) The computer-accessible medium as recited in claim 209, wherein the code portion for generating a first encryption key at the redirector host system further comprises a code portion for generating a public key.

215. (New) The computer-accessible medium as recited in claim 214, wherein the code portion for generating a first decryption key at the redirector host system further comprises a code portion for generating a private key.

216. (New) The computer-accessible medium as recited in claim 209 further comprising:

a code portion for receiving the encrypted new data item at the user's mobile device; and

a code portion for decrypting the encrypted new data item to recover the new data item using a cipher algorithm and the first decryption key.

217. (New) The computer-accessible medium as recited in claim 216 further comprising a code portion for storing the new data item within a memory of the user's mobile device.

218. (New) The computer-accessible medium as recited in claim 216 further comprising:

a code portion for generating a second decryption key at the redirector host system;

a code portion for storing the second decryption key at the redirector host system;

a code portion for generating a second encryption key at the redirector host system; and

a code portion for forwarding the second encryption key from the redirector host system to the user's mobile device using the secure communications link.

219. (New) The computer-accessible medium as recited in claim 218, wherein the code portions for generating a second encryption key at the redirector host system and generating a second decryption key at the redirector host system further comprise a code portion for generating a shared key.

220. (New) The computer-accessible medium as recited in claim 218, wherein the code portions for generating a second encryption key at the redirector host system and generating a second decryption key at the redirector host system further comprise a code portion for generating the second encryption key and the second decryption key according to a symmetric key encryption scheme.

221. (New) The computer-accessible medium as recited in claim 218, wherein the code portion for generating a second encryption key at the redirector host system further comprises a code portion for generating a public key.

222. (New) The computer-accessible medium as recited in claim 221, wherein the code portion for generating a second decryption key at the redirector host system further comprises a code portion for generating a private key.

223. (New) The computer-accessible medium as recited in claim 218 further comprising:

a code portion for preparing a reply data item at the user's mobile device that is related to the new data item;

a code portion for encrypting the reply data item at the mobile device to form an encrypted reply data item using a cipher algorithm and the second encryption key; and

a code portion for transmitting the encrypted reply data item to the redirector host system.

224. (New) The computer-accessible medium as recited in claim 223 further comprising:

a code portion for receiving the encrypted reply data item at the redirector host system;

a code portion for decrypting the encrypted reply data item to recover the reply data item; and

a code portion for transmitting the reply data item to the messaging host system.

225. (New) The computer-accessible medium as recited in claim 224 further comprising a code portion for transmitting the reply data item to a destination system using an electronic address associated with the user at the messaging host system, wherein reply data items created at either the messaging host system or the user's mobile device share the electronic address as an originating address.